PATENT
32860-000707/US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: **NEW APPLICATION**

Filing Date: March 12, 2004

Applicant(s): Thomas BIRKHOELZER et al.

Title: USER OBJECTS FOR AUTHENTICATING THE USE OF ELECTRONIC DATA

PRIORITY LETTER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

March 12, 2004

Dear Sirs:

Pursuant to the provisions of 35 U.S.C. 119, enclosed is/are a certified copy of the following priority document(s).

Application No.	Date Filed	Country
10311327.4	March 14, 2003	GERMANY

In support of Applicants' priority claim, please enter this document into the file.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____
Donald J. Daley, Reg. No. 34,313

DJD/bof

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

Enclosure

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	103 11 327.4
Anmeldetag:	14. März 2003
Anmelder/Inhaber:	Siemens Aktiengesellschaft, 80333 München/DE
Bezeichnung:	Nutzer-Objekte zur Authentifizierung der Nutzung elektronischer Daten
IPC:	G 06 F 17/40

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 19. Februar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Remus

A 9161
06/00
EDV-L

Beschreibung

Nutzer-Objekte zur Authentifizierung der Nutzung elektronischer Daten

Die Erfindung betrifft eine elektronische Datenverarbeitungseinrichtung zum Bearbeiten, Speichern und Auslesen von elektronischen Daten durch unterschiedliche Anwender, denen unterschiedliche Daten-Zugriffsrechte erteilt werden und deren Daten-Zugriffe dokumentiert werden. Die Erfindung betrifft außerdem ein Verfahren zum Betrieb einer Datenverarbeitungseinrichtung sowie ein Speichermedium mit Informationen zur Ausführung eines solchen Verfahrens auf einer Datenverarbeitungseinrichtung.

Text- und Bilddaten, insbesondere medizinisch relevante Daten wie Befunde, diagnostische Bilder oder Patientendaten, werden vermehrt elektronisch abgelegt und gehandhabt. Die elektronische Handhabung erfordert besondere Maßnahmen, um Datenzugriffe und Datenveränderungen nachvollziehbar zu machen. Insbesondere im Gesundheitswesen sind viele elektronische Daten als vertraulich einzustufen und Datenschutzbestimmungen fordern, dass jeder Nutzer elektronischer Daten eindeutig identifiziert und authentifiziert wird. Jeder Datenzugriff bzw. jede Nutzung der Daten muss eindeutig unter Angabe des Nutzers dokumentiert werden („auditing") und der Zugriff auf Daten von Patienten darf nur authentifizierten Nutzern gewährt werden („access control"). Damit repräsentiert die Identifikation die eindeutige, individuelle Kennung des Nutzers, während mit Authentifizierung die Zulassung bestimmter Datenzugriffsrechte für den Nutzer gemeint ist. Die Authentifizierung bedeutet also eine Autorisierung des Nutzers für bestimmte Datenzugriffsrechte. Die Authentifizierung setzt grundsätzlich eine Identifizierung voraus.

Daraus ergeben sich die folgenden Forderungen. Für die eindeutige Dokumentation ist es notwendig, dass jeder Nutzer in-

dividuell identifiziert werden kann. Für den Schutz der Daten vor nicht-autorisiertem Zugriff sind Mechanismen in unterschiedlich tiefen Software-Ebenen denkbar, wobei die Umgehbarkeit dieser Mechanismen von der jeweiligen Tiefe der Software-Ebene abhängt. Mechanismen, die in tieferen Software-Ebenen ablaufen, das bedeutet im Extremfall auf Betriebs-System-Ebene, lassen weniger Umgehungsmöglichkeiten zu und gewährleisten daher einen sichereren Zugriffschutz. Daher werden Zugriffsrechte bei der Handhabung sicherheitskritischer oder medizinisch relevanter Daten, insbesondere personenbezogener Daten und Patientendaten, soweit wie möglich auf Ebene des Betriebs-Systems realisiert. Dies erfordert, dass ein Nutzer, der umfassende Zugriffsrechte genießen soll, als Betriebs-System-Nutzer an einem System angemeldet sein muss, welches Zugriff auf die Daten gewähren kann. Ein Nutzer, der weniger umfassende Zugriffsrechte genießen soll, muss dagegen lediglich als Anwendungs-Nutzer bei der Anwendungs-Software angemeldet sein.

Ein mögliches System zur Handhabung elektronischer Daten könnte ein medizinischer Arbeitsplatz sein, zum Beispiel eine sogenannte Modalität, an der Befund- und Bilddaten erfasst und bearbeitet werden können. An einem solchen Arbeitsplatz arbeiten typischerweise mehrere Personen in enger zeitlicher Abfolge, die jeweils zwischen Betreuung des Patienten und Bedienung des Geräts in schnellem Takt hin- und herwechseln. An ein und demselben Arbeitsplatz arbeiten also mehrere Nutzer in schnellem Wechsel und betreuen mehrere Patienten. Es ist offensichtlich, dass das Wechseln zwischen verschiedenen Nutzern und verschiedenen Patienten unter Gesichtspunkten der Rationalisierung und Ökonomie der Arbeitsabläufe möglichst schnell erfolgen sollte.

Andere Systeme zur Handhabung vertraulicher elektronischer Daten sind zum Beispiel in der Forschung, im Finanzwesen, in der Juristerei oder in demographischen Fragen Verwendung fin-

den. Grundsätzlich sind personenbezogene und geheimhaltungsbedürftige Daten gleichermaßen als vertraulich anzusehen.

Da die fraglichen Daten im allgemeinen als in besonderem Maße schutzbedürftig angesehen werden, wird eine möglichst sichere Authentifizierung der Nutzer gefordert. Nach dem oben gesagten sollte die Authentifizierung also auf Betriebs-System-Ebene realisiert sein. Das hat zur Folge, dass ein Wechsel zwischen verschiedenen Nutzern nur durch Neuanmeldung am Betriebs-System erfolgen kann. Die Neuanmeldung am Betriebs-System ist in den heute verwendeten Systemen jedoch sehr zeitaufwändig, da sie jedes mal einen Neustart des Betriebs-Systems erfordert und darüber hinaus auch jedes Mal das Beenden und Neustarten des Anwendungs-Programms verlangt, mit dem die Daten bearbeitet werden. Durch die zeitaufwändigen Neustarts wird die Realisierung einer möglichst großen Zugriffs-Sicherheit an Arbeitsplätzen, die im häufigen und schnellen Wechsel benutzt werden sollen, zu zeitaufwändig und daher in der häufig mit Zeitdruck konfrontierten Praxis nicht akzeptabel.

Herkömmliche medizinische und andere mit vertraulichen Daten arbeitenden Arbeitsplätze weisen daher Daten-Sicherheitssysteme auf, die in aller Regel die Mehrfachnutzung des Arbeitsplatzes entweder von vorneherein verhindern oder die mutwillige Umgehungen des Sicherheitssystems im täglichen Gebrauch unter Zeitdruck provoziert, indem verschiedene Nutzer dazu verleitet sind, unter Verzicht auf jeweilige Neuanmeldung am System unter Verwendung von ein und derselben gemeinsamen System-Anmeldung zu arbeiten. Die Benutzung einer gemeinsamen System-Anmeldung hat außerdem zur Folge, dass die Dokumentation von Nutzerdaten im Zusammenhang mit Zugriffen auf die sicherheitskritischen Daten erschwert wird, da das System verschiedene Nutzer, die mit derselben System-Anmeldung arbeiten, nicht individuell identifizieren kann.

Die Aufgabe der Erfindung besteht darin, ein System zum Bearbeiten, Speichern und Auslesen elektronischer Daten anzugeben, das bei unverminderter Datensicherheit schnellere Nutzer-Wechsel ermöglicht, in dem die vollständige Identifikation zu Dokumentationszwecken sowie zur korrekten Authentifizierung einzelner Nutzer ermöglicht wird.

Die Erfindung erreicht dieses Ziel durch eine Datenverarbeitungseinrichtung, durch ein Verfahren zum Betrieb einer solchen Einrichtung sowie durch ein Speichermedium mit Informationen zur Ausführung eines solchen Verfahrens auf einer Datenverarbeitungseinrichtung mit den Merkmalen der unabhängigen Patentansprüche.

Die Erfindung beruht auf der Erkenntnis, dass verschiedene Nutzer eines mit vertraulichen elektronischen Daten arbeitenden Arbeitsplatzes häufig dem gleichen Authentifizierungs-Level angehören, d.h. gleiche Zugriffsrechte auf die fraglichen Daten haben. Im Kontext des Datenschutzes im Gesundheitswesen sind die Nutzer in einem gemeinsamen Authentifizierungs-Level z.B. als ein behandelndes Team anzusehen, dessen Zugriffsrechte als Team- oder Gruppenzugriffsrechte definiert sind.

Bislang muss ein Nutzer am System als einheitliches, individuelles Nutzer-Objekt angemeldet werden, das zu Dokumentations- und Authentifizierungszwecken verwendet wird. Die Erfindung entkoppelt die herkömmliche Verbindung von Identifikations- und Authentifizierungs-Objekt. Stattdessen verwendet sie ein individuelles Dokumentations-Nutzer-Objekt, das Information zur Identifikation eines Nutzers beinhaltet, und ein davon getrenntes Authentifizierungs-Nutzer-Objekt, das einen bestimmten Authentifizierungs-Level definiert. Das Authentifizierungs-Nutzer-Objekt kann nicht-individuell an alle Nutzer eines identischen Authentifizierungs-Levels vergeben werden und in diesem Sinne als Gruppen-Nutzer-Objekt für Nutzergruppen angesehen werden.

Durch die Verwendung der getrennten Nutzer-Objekte kann ein Wechsel zwischen Nutzern eines gemeinsamen Authentifizierungs-Levels, z.B. eines behandelnden Teams, durch einen Wechsel des individuellen Dokumentations-Nutzer-Objekts vollzogen werden, ohne zwangsläufig auch das Betriebs-System wegen eines damit verbundenen Wechsels des Authentifizierungs-Nutzer-Objekts neu starten zu müssen. Zum Beispiel kann der Wechsel zwischen Nutzer-Objekten, die einer gemeinsamen Nutzer-Gruppe angehören, auf Ebene einer medizinischen oder personenbezogenen Anwendungs-Software zur Datenbearbeitung vollzogen werden. Erst beim Wechsel zwischen Nutzern unterschiedlicher Nutzer-Gruppen muss auch ein Wechsel des Authentifizierungs-Levels vollzogen werden, also eine Ab- und Wieder-Anmeldung auf Ebene des Betriebs-Systems.

Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der abhängigen Patentansprüche.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand von Figuren näher erläutert. Es zeigen dabei:

FIG 1 Schematisch dargestellte Datenverarbeitungseinrichtung,

FIG 2 Flussdiagramm,

FIG 3 Nutzer-Ebenen.

Figur 1 zeigt die Architektur einer bevorzugten Ausführungsform der elektronischen Datenverarbeitungseinrichtung. Zentrales Element dieser Datenverarbeitungseinrichtung, die z.B. ein medizinischer Arbeitsplatz, eine Forschungs-Workstation oder eine Finanz-Terminal sein kann, ist ein Computer **1**, der über ein Eingabegerät **9**, z.B. eine Tastatur, und ein Ausgabegerät **11**, z.B. einen Bildschirm, verfügt.

Der Computer 1 hat Zugriff auf einen Datenspeicher 3, in dem personenbezogene oder medizinisch relevante, also als vertraulich einzustufende elektronische7 Daten abgelegt sind. Auf dem Computer 1 läuft in üblicher Weise ein Betriebs-System, das zur Konfigurierung der Hardware und zum Betrieb des Computers 1 erforderlich ist. Weiter läuft auf dem Computer 1 ein Anwendungsprogramm, das zur Handhabung der vertraulichen Bild-, Text- oder Metadaten geeignet ist. Das Anwendungsprogramm kann beispielsweise der Eingabe von Patientendaten dienen, der Eingabe von medizinischen Befunden oder Begutachtungen, der Bearbeitung diagnostischer Bilddaten oder der Erfassung personenbezogener Informationen. Als Nutzer des Programms können medizinisches Fachpersonal oder Patienten ebenso wie Verwaltungspersonal, Techniker, Kauflaute, Forscher oder Finanz-Fachleute in Frage kommen. Die Computer 1 erlaubt die Verarbeitung der elektronischen Daten, wobei mit Verarbeitung das Erzeugen, Speichern, Verändern, Löschen oder Lesen sowie jeglicher sonstige Datenzugriff gemeint sein soll.

Der Computer 1 hat weiter Zugriff auf einen Dokumentations-Speicher 5, der sämtliche Zugriffe auf die Daten im Datenspeicher 3 dokumentiert. Zu diesem Zweck werden Informationen über die Art des Zugriffs, die zugegriffenen Daten und den zugreifenden Nutzer abgelegt, wobei als Zugriff auf die Daten nicht nur eine Veränderung sondern auch deren bloße Betrachtung aufzufassen ist.

Der Computer 1 ist außerdem mit einem Authentifizierungs-Speicher 7 verbunden, der entweder in direkter Verbindung oder entfernt vom Computer 1 an zentraler Stelle angeordnet sein kann und über eine Datenfernübertragungs-Verbindung 8 zugreifbar ist. Der Authentifizierungs-Speicher 7 enthält Informationen, die es erlauben, einen Nutzer des Computers 1 bzw. des gesamten Datenverarbeitungs-Systems als Nutzer zu identifizieren, ihm ein Nutzer-Objekt zuzuordnen, als das er am System angemeldet werden kann, und festzustellen, welcher

Nutzer-Gruppe das Nutzer-Objekt angehört. Die Nutzer-Gruppe enthält dabei Informationen, die den Authentifizierungs-Level definieren, der für das Nutzer-Objekt gilt. Mit anderen Worten können dem Nutzer-Objekt über die Zugehörigkeit zu einer Nutzer-Gruppe Zugriffsrechte zugeordnet und erteilt werden und damit seine Authentifizierung vorgenommen werden.

Um einen Nutzer des Systems identifizieren und ihm ein Nutzer-Objekt zuordnen zu können, muss der Computer **1** Informationen über den Nutzer abfragen, die er mit den Informationen im Authentifizierungs-Speicher **7** vergleichen kann. Da im Ergebnis dieser Identifizierung Dokumentationsdaten erzeugt und der Authentifizierungs-Level des Nutzers festgelegt werden, sind die abzufragenden Informationen selbst in besonderem Maße vertraulich zu handhaben und zu schützen. Die Abfrage kann daher in Form einer Passwort-Abfrage erfolgen. Die Verwendung von Passwörtern hat bekanntlich den Nachteil, dass ausreichend sichere Passwörter in aller Regel lang, schwer zu merken und umständlich einzugeben sind. Dies erschwert die Benutzung und insbesondere den schnellen Wechsel von Nutzern am System. Praktikablere Alternativen zu einer Passwortabfrage bestehen darin, über eine Kamera **13** biometrische Daten des Nutzers, z.B. die Gestalt seiner Iris, zu erfassen, über einen Schlüssel-Leser **15** einen Nutzer-individuellen elektronischen oder mechanischen Schlüssel abzutasten oder über einen Chipkarten-Leser **17** eine Nutzer-individuelle Chipkarte abzufragen. Die vorgeschlagenen Sicherheitssysteme ermöglichen eine sichere und für den Nutzer unaufwändige Identifikation, wobei insbesondere die Abfrage biometrischer Daten als besonders Nutzer-komfortabel und täuschungssicher gilt.

Der Authentifizierungs-Speicher **7** kann in vorteilhafter Weise entfernt vom Arbeitsplatz zentral positioniert sein. Auf diese Weise kann er als Daten-Server für ein ganzes Gebäude, z.B. ein Krankenhaus, Büro-Gebäude oder Gebäude-übergreifend eingesetzt werden. Bei zentraler Positionierung als Authentifizierungs-Server kann er nach Art eines Trust-Centers mit

asymmetrischen Schlüsselsystemen arbeiten. Bei Verwendung eines asymmetrischen Schlüsselsystems mit öffentlichem und privatem Schlüssel erübrigt sich auch das Erfordernis, die Datenfernübertragungs-Verbindung **8** verschlüsselt zu betreiben. Selbstverständlich sind ausreichende Schutzmaßnahmen, wie Firewalls, zum Schutz der Daten im Datenspeicher **3** bzw. im ganzen System vorzusehen.

Die Verwendung eines zentralen Authentifizierungs-Servers erhöht die Portabilität der Daten und ermöglicht außerdem die Verwendung von Expertensystemen mit Zugriff auf die Daten von örtlich getrennt arbeitenden Experten, da die Dokumentation und Authentifizierung nicht lokal eingeschränkt wäre. Außerdem könnten Normen hinsichtlich der verschiedenen Authentifizierungs-Level zentral definiert und vorgegeben werden, um sie im gesamten Datensystem, etwa für das gesamte Gesundheitswesen, einheitlich einsetzen zu können.

Das Betriebs-System, das auf dem Computer **1** läuft, dient in bekannter Weise der hardwaremäßigen Konfigurierung des Computers. Es entscheidet darüber, welche Hardware-Komponenten verfügbar sind und durch welche Nutzer auf diese Komponenten zugegriffen werden kann. Dadurch ist es in der Lage, die Benutzung der Hardware und damit auch der in der Hardware gespeicherten Daten Nutzer-abhängig freizugeben, zu sperren oder zu autorisieren. Darüber hinaus dient das Betriebs-System als Plattform, auf der Anwendungsprogramme laufen können, wobei es zwangsläufig auch die Zugriffsrechte für die Anwendungsprogramme selbst autorisiert. Da die Anwendungsprogramme auf dem Betriebs-System aufgesetzt arbeiten, ist deren Beenden und Starten bei laufendem Betriebs-System möglich. Das Verändern des gültigen Authentifizierungs-Levels ist dagegen bei maximaler Datensicherheit nur durch Beenden und Neustarten des Betriebs-Systems möglich.

Figur 2 zeigt als Flussdiagramm die Verfahrens-Schritte, nach denen die Erfindung arbeitet. Das Flussdiagramm zeigt die Ar-

beitsabläufe, die das Betriebs-System und die Anwendungsprogramme ausführen. In Schritt **31** meldet sich zunächst ein Anwender für die Nutzung des Systems, z.B. des medizinischen Arbeitsplatzes, an. Die Anmeldung erfolgt dabei in bekannter Weise durch Eingabe einer Benutzerkennung über eine Tastatur oder ein anderes geeignetes Eingabegerät. Die Benutzerkennung gleicht einem Login oder Anmeldungs-Namen und vermittelt keinerlei Datensicherheit.

In Abhängigkeit von der Anmeldung eines Anwenders erfolgt in Schritt **33** eine Sicherheitsabfrage. Die Sicherheitsabfrage dient der täuschungssicheren Identifizierung eines Anwenders und gleicht daher der Eingabe eines Benutzer-Passworts. Sie kann als Passwort-Eingabe über eine Tastatur erfolgen, statt dessen können jedoch auch biometrische Daten des Anwenders über eine Kamera ermittelt oder ein mechanischer oder elektronischer Schlüssel oder eine Chipkarte über ein mit dem System verbundenes Abfragegerät abgetastet werden.

Je nach Art der Sicherheitsabfrage in Schritt **33** kann die Eingabe einer Benutzerkennung im vorhergehenden Schritt **31** verzichtbar sein. Beispielsweise kann durch eine automatisch durchgeführt biometrische Messung eine vollständige und sichere Identifikation ohne Zutun des Nutzers in Schritt **31** durchgeführt werden. Die Verwendung eines ausreichend sicheren Schlüssels kann gleichzeitig zur Erkennung des Benutzers und zur Verifizierung, also als eigentliche Sicherheitsabfrage, ausreichend sein. Dies erleichtert insbesondere häufige Benutzerwechsel am System, weil umständliche Tastatureingaben entfallen können.

In Schritt **35** wird der zuvor erkannte Anwender durch ein auf Ebene des Betriebs-Systems arbeitendes Programm als Nutzer-Objekt identifiziert. Das System greift dazu auf einen Datenbestand zu, der eine Erkennung von Anwendern anhand der in der Sicherheitsabfrage ermittelten Daten ermöglicht. Dieser Datenbestand kann sowohl innerhalb des Systems gespeichert

als auch über entfernt zugreifbare Daten, z.B. über das Internet, zugreifbar sein. Es können auch lokale und nichtlokale Daten parallel verwendet werden.

Im nächsten Schritt **37** wird festgestellt, welcher Nutzer-Gruppe das zuvor identifizierte Nutzer-Objekt angehört. Dazu wird auf Daten zugegriffen, die ebenfalls lokal oder nichtlokal gespeichert sein können. Die Datenbestände zur Identifizierung von Nutzer-Objekten und zu deren Zuordnung zu Nutzer-Gruppen können sowohl im selben als auch in getrennten Datenspeichern abgelegt sein.

In Schritt **39** wird überprüft, ob die Nutzer-Gruppe des aktuell am System anzumeldenden Nutzer-Objekts derjenigen des zuvor angemeldeten Nutzer-Objekts entspricht, oder ob das Nutzer-Objekt einer anderen Nutzer-Gruppe angehört. Stimmen die aktuell anzumeldende und die zuvor angemeldete Nutzer-Gruppe überein, startet das System in Schritt **49** das vom Anwender gewünschte Anwendungsprogramm. Andernfalls wird ein Neustart des Systems erforderlich, da der Wechsel der Nutzer-Gruppe mit einem Wechsel des Authentifizierungs-Levels verbunden ist, der nur durch Änderungen auf Ebene des Betriebs-Systems realisiert wird kann.

Zu diesem Zweck wird in Schritt **41** die gegenwärtige Konfiguration laufender Anwendungsprogramme zwischengespeichert und in Schritt **43** werden die Anwendungsprogramme beendet. In Schritt **45** wird der gegenwärtige Status des Betriebs-Systems zwischengespeichert und in Schritt **47** das Betriebs-System beendet und neu gestartet.

Durch die zwischengespeicherten Daten hinsichtlich des Status des Betriebs-Systems und der Konfiguration der Anwendungen kann nach dem Neustart des Betriebs-Systems die vorherige Arbeitsplatz-Konfiguration wiederhergestellt werden. Dabei kann der zuvor zur Anmeldung identifizierte Anwender automatisch am Betriebs-System angemeldet und der zugehörige Authentifi-

zierungs-Level eingestellt werden. Es kann aber auch eine erneute Anmeldung des Anwenders in Schritt **31** verlangt werden. Dazu muss die Sicherheitsabfrage in Schritt **33**, die Identifizierung als Nutzer-Objekt in Schritt **35** und die Zuordnung zu einer Nutzer-Gruppe in Schritt **37** wiederholt werden. Nach erfolgreicher Authentifizierung wird in Schritt **49** die vorherige Konfiguration der Anwendungsprogramme oder eine gewünschte Anwendung gestartet.

In Schritt **51** stellt das Anwendungsprogramm fest, ob das aktuell angemeldete Nutzer-Objekt mit dem neu anzumeldenden übereinstimmt, oder ob ein Wechsel erfolgt ist. Falls ein Wechsel erfolgt ist, wird in Schritt **53** auf Ebene des Anwendungsprogramms das nun gültige Nutzer-Objekt neu eingetragen und kann nun zu Dokumentationszwecken jederzeit abgerufen werden, ansonsten bleibt das vorherige Nutzer-Objekt aktiv.

In Schritt **55** erfolgt die Dokumentation der Daten-Zugriffe des Anwenders auf die vertraulichen Daten. Dabei wird dokumentiert, welcher Anwender mittels welchen Anwendungsprogramms wann auf welche Daten zugreift. Außerdem wird die Art des Datenzugriffs dokumentiert, d.h. es wird festgehalten, ob eine Bearbeitung oder lediglich eine Betrachtung der Daten erfolgt ist.

Anhand des Flussdiagramms in Figur **2** wird deutlich, dass die Erfindung den Wechsel von Anwendern am System vereinfacht. In herkömmlichen Systemen müssen die Schritte **41** bis **49** zum Neustart von Betriebs-Systemen und Anwendungsprogrammen bei jedem Nutzer-Wechsel abgearbeitet werden, wobei insbesondere der Schritt **47**, in dem das Betriebs-System neu gestartet wird, besonders zeitaufwendig ist. Die Erfindung dagegen ermöglicht es, auf diese Schritte immer dann zu verzichten, wenn festgestellt wird, dass der Authentifizierungs-Level bzw. das Authentifizierungs-Nutzer-Objekt des neu anzumeldenden Anwenders mit demjenigen des aktuell angemeldeten Anwenders übereinstimmen. Immer dann wird auf den Neustart des Be-

triebs-Systems verzichtet und höchstens ein Neustart des Anwendungsprogramms zum Wechsel des Dokumentations-Nutzer-Objekts durchgeführt.

In aller Regel wird jedoch ein Neustart des Anwendungsprogramms zum Wechsel des Dokumentations-Nutzer-Objekts verzichtbar sein. Stattdessen wird lediglich innerhalb der Anwendung das neue Nutz-Objekt verzeichnet.

Figur 3 verdeutlicht die Trennung zwischen Betriebs-System- und Anwendungs-Ebene, die sich die Erfindung zunutze macht. Das Betriebs-System **71** befindet sich in Figur **3** auf der Ebene oberhalb der gestrichelten Linie, die von der Ebene der Anwendungsprogramme **73** unterhalb der gestrichelten Linie getrennt ist.

Das Betriebs-System **71** ist für die Konfigurierung der Hardware der Datenverarbeitungseinrichtung zuständig und für die Identifizierung und Authentifizierung eines System-Nutzers. Dazu weist das Betriebs-System eine Authentifizierungs-Instanz **75** auf, die entweder Teil des Betriebs-Systems ist oder auf Ebene des Betriebs-Systems arbeitet, um je nach Nutzer-Objekt einen anderen Authentifizierungs-Level vorgeben zu können. Die zu einem Authentifizierungs-Level gehörige Hardware-Konfiguration und der jeweilige Umfang an Zugriffsrechten sind dabei in Nutzer-Gruppen **77** definiert. Jede Nutzer-Gruppe **77** definiert einen eigenen Authorisierungs-Level und eine eigene Hardware-Konfiguration. Ein Wechsel des Authentifizierungs-Nutzer-Objekts und damit der Nutzer-Gruppe **77** findet auf Ebene des Betriebs-Systems **71** statt.

Auf der Ebene der Anwendungsprogramme **73** erfolgen die entsprechend dem vergebenen Authentifizierungs-Level erlaubten Datenzugriffe und werden durch die Dokumentations-Instanz **79** dokumentiert. Die Dokumentations-Instanz **79** zeichnet auf, welcher Anwender wann auf welche Daten auf welche Art zugegriffen hat. Es werden sowohl Datenzugriffe zur Veränderung

der Daten als auch solche zur bloßen Betrachtung der Daten dokumentiert. Die Umfänglichkeit der Dokumentation entspricht mindestens den herrschenden, für die Daten vorgegeben gesetzlichen Vorgaben. Die Dokumentations-Instanz **79** benötigt zur Aufzeichnung des Anwenders, der auf Daten zugreift, Informationen zu dessen Identifikation. Diese Informationen sind durch das jeweils angemeldete Dokumentations-Nutzer-Objekt **81** gegeben, dessen Kennung als Urheber jedes Datenzugriffs gespeichert wird.

Die Nutzer-Objekte **81** sind jeweils Teil einer Nutzer-Gruppe **77**. Ein Wechsel des Nutzer-Objekts **81** muss nicht mit einem Wechsel des Authentifizierungs-Levels einhergehen, d.h. er kann ohne Wechsel der Nutzer-Gruppe **77** und allein auf Ebene des Anwendungsprogramms **73** vollzogen werden. Um dies zu verdeutlichen, sind in Figur **3** jeweils mehrere Nutzer-Objekte **81** innerhalb einer Nutzer-Gruppe **77** auf Ebene des Anwendungs-Programms dargestellt. Es ist aus der Darstellung ersichtlich, dass nur ein Wechsel zu einem Nutzer-Objekt **81** in einer anderen Nutzer-Gruppe **77** auch deren Wechsel und damit eine Änderung auf Ebene des Betriebs-Systems erforderlich macht. Nur in solchen Fällen wird ein Neustart des Betriebs-Systems **71** erforderlich, der dann mit einem Wechsel des Authentifizierungs-Levels einhergehen kann, was zur Erteilung eines geänderten Umfangs an Zugriffsrechten durch die Authentifizierungs-Instanz **75** an das Anwendungsprogramm **73** führt.

Der Umfang der Daten-Zugriffs-Rechte wird damit durch die Betriebs-System-Ebene vorgegeben, während die Dokumentation von Datenzugriffen ausschließlich auf Anwendungsprogramm-Ebene erfolgt.

Patentansprüche

1. Elektronische Datenverarbeitungseinrichtung (1) zum Verarbeiten elektronischer Daten durch wechselnde Nutzer, auf der ein Betriebs-System zur Konfiguration der Datenverarbeitungseinrichtung und ein Anwendungs-Programm zur Bearbeitung der Daten läuft, mit einem Daten-Speicher (3) zur Speicherung der Daten, mit einem Dokumentations-Speicher (5) zur Speicherung von Dokumentations-Daten zur Dokumentation eines Zugriffs auf die Daten, mit einem Nutzer-Objekt-Speicher (7) zur Speicherung von Nutzer-Objekten zur Authentifizierung und Dokumentation eines Zugriffs auf die Daten,
d a d u r c h g e k e n n z e i c h n e t , dass durch den Nutzer-Objekt-Speicher (7) Dokumentations-Nutzer-Objekte (81) speicherbar sind, die auf Ebene des Anwendungs-Programms (73) zur Dokumentation eines Zugriffs auf die Daten im Dokumentations-Speicher (5) speicherbar sind, und ein Authentifizierungs-Nutzer-Objekt (77), dem auf Ebene des Betriebs-Systems (71) ein Recht zum Zugriff auf die Daten zuordenbar ist, und dem mehrere Dokumentations-Nutzer-Objekte (81) zuordenbar sind, die dadurch für dieses Recht authentifiziert sind.

2. Elektronische Datenverarbeitungseinrichtung (1) nach Anspruch 1
d a d u r c h g e k e n n z e i c h n e t , dass ein Nutzer vor einem Zugriff auf die Daten durch eine Sicherheitsabfrage identifiziert werden muss, und dass einem Nutzer in Abhängigkeit vom Ergebnis der Sicherheitsabfrage ein Dokumentations-Nutzer-Objekt (81) und ein Authentifizierungs-Nutzer-Objekt (77) zuordenbar ist.

3. Elektronische Datenverarbeitungseinrichtung (1) nach Anspruch 2
d a d u r c h g e k e n n z e i c h n e t , dass zur Sicherheitsabfrage ein Mittel (13) zur Abfrage biometrischer Daten und/oder ein Mittel (15) zur Abfrage eines mechanischen

und/oder elektronischen Schlüssels oder ein Mittel (17) zur Abfrage einer Chip-Karte vorgesehen ist.

4. Elektronische Datenverarbeitungseinrichtung (1) nach einem der vorhergehenden Ansprüche d a d u r c h g e k e n n z e i c h n e t , dass der Nutzer-Objekt-Speicher (7) über eine zur Fernübertragung von Daten geeignete Verbindung mit der Datenverarbeitungseinrichtung (1) verbunden ist.

5. Verfahren zum Verarbeiten elektronischer Daten durch einen Nutzer mittels einer elektronischen Datenverarbeitungseinrichtung (1), auf der ein Betriebs-System (71) zur Konfiguration der Datenverarbeitungseinrichtung (1) und ein Anwendungs-Programm (73) zur Bearbeitung der Daten läuft, d a d u r c h g e k e n n z e i c h n e t , dass in einem ersten Schritt (35) ein Nutzer als Dokumentations-Nutzer-Objekt (81) identifiziert wird, dass in einem zweiten Schritt (37) der Nutzer als Authentifizierungs-Nutzer-Objekt (77) identifiziert wird, dass in einem dritten Schritt (47) dem Authentifizierungs-Nutzer-Objekt (77) ein Recht zum Zugriff auf Daten auf Ebene des Betriebs-Systems (71) zugeordnet wird, dass in einem vierten Schritt (55) auf Ebene des Anwendungs-Programms (73) Zugriffe auf Daten zu Dokumentations-Zwecken in Verbindung mit einem Dokumentations-Nutzer-Objekt (81) gespeichert werden, und dass mehrere Nutzer durch dasselbe Authentifizierungs-Nutzer-Objekt (77) identifizierbar sind und dadurch für dasselbe Recht zum Zugriff auf Daten authentifizierbar sind.

6. Speichermedium, auf dem Information gespeichert ist, und das in Wechselwirkung mit einer elektronischen Datenverarbeitungseinrichtung (1) treten kann, um das Verfahren gemäß Anspruch 5 auszuführen.

Zusammenfassung

Nutzer-Objekte zur Authentifizierung der Nutzung medizinischer Daten

Die Erfindung betrifft eine elektronische Datenverarbeitungseinrichtung (1) zum Verarbeiten elektronischer Daten durch wechselnde Nutzer. Sie betrifft weiter ein entsprechendes Verfahren und ein Speichermedium mit Informationen zur Ausführung dieses Verfahrens auf einer Datenverarbeitungseinrichtung. Auf der Datenverarbeitungseinrichtung (1) läut ein Betriebs-System (71) zur Konfiguration der Datenverarbeitungseinrichtung und ein Anwendungs-Programm (73) zur Bearbeitung der Daten. Sie weist einen Daten-Speicher (3) zur Speicherung der Daten und einen Dokumentations-Speicher (5) zur Speicherung von Dokumentations-Daten zur Dokumentation eines Zugriffs auf die Daten auf. Sie weist weiter einen Nutzer-Objekt-Speicher (7) zur Speicherung von Nutzer-Objekten zur Authentifizierung und Dokumentation auf. Gemäß der Erfindung beinhaltet der Nutzer-Objekt-Speicher (7) Dokumentations-Nutzer-Objekte (81), die auf Ebene des Anwendungs-Programms (73) zur Dokumentation eines Zugriffs auf die Daten im Dokumentations-Speicher (5) speicherbar sind, und ein Authentifizierungs-Nutzer-Objekt (77), dem auf Ebene des Betriebs-Systems (71) ein Recht zum Zugriff auf die Daten zuordenbar ist, und dem mehrere Dokumentations-Nutzer-Objekte (81) zuordenbar sind, die dadurch für dieses Recht authentifiziert sind.

FIG 2

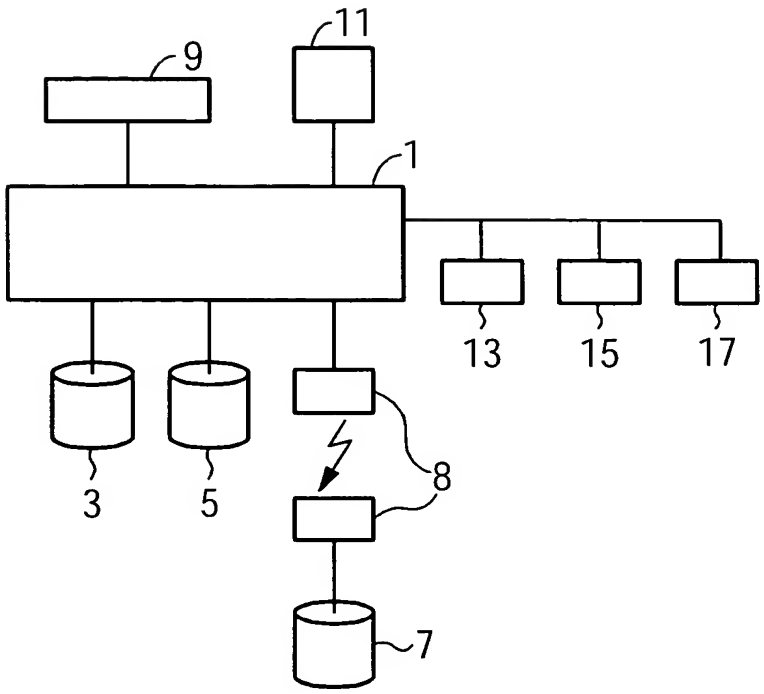

FIG 1

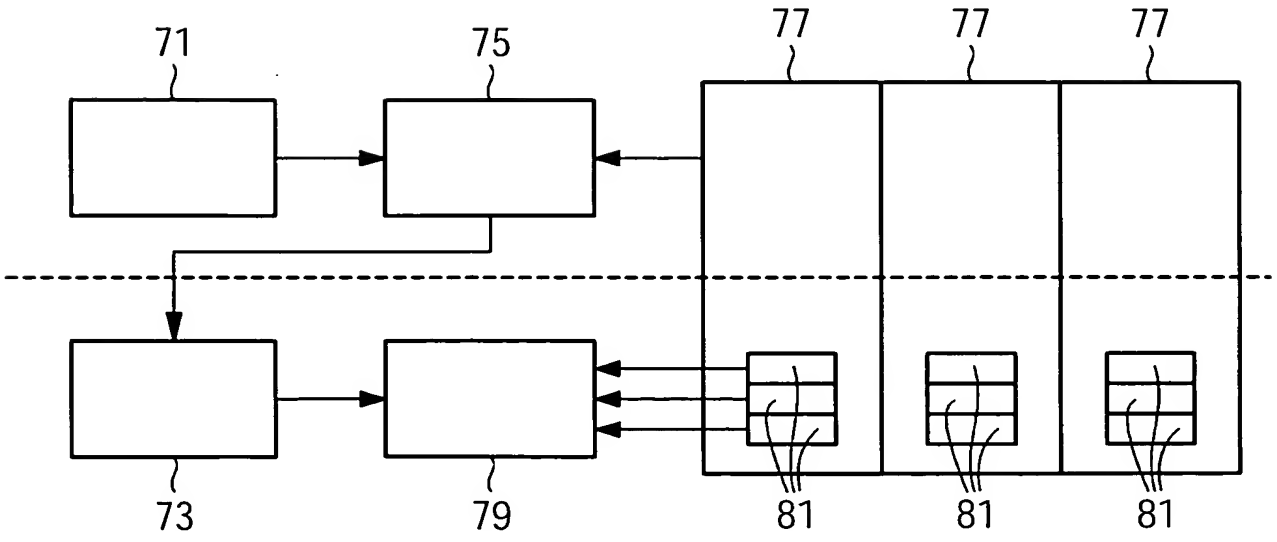

FIG 3

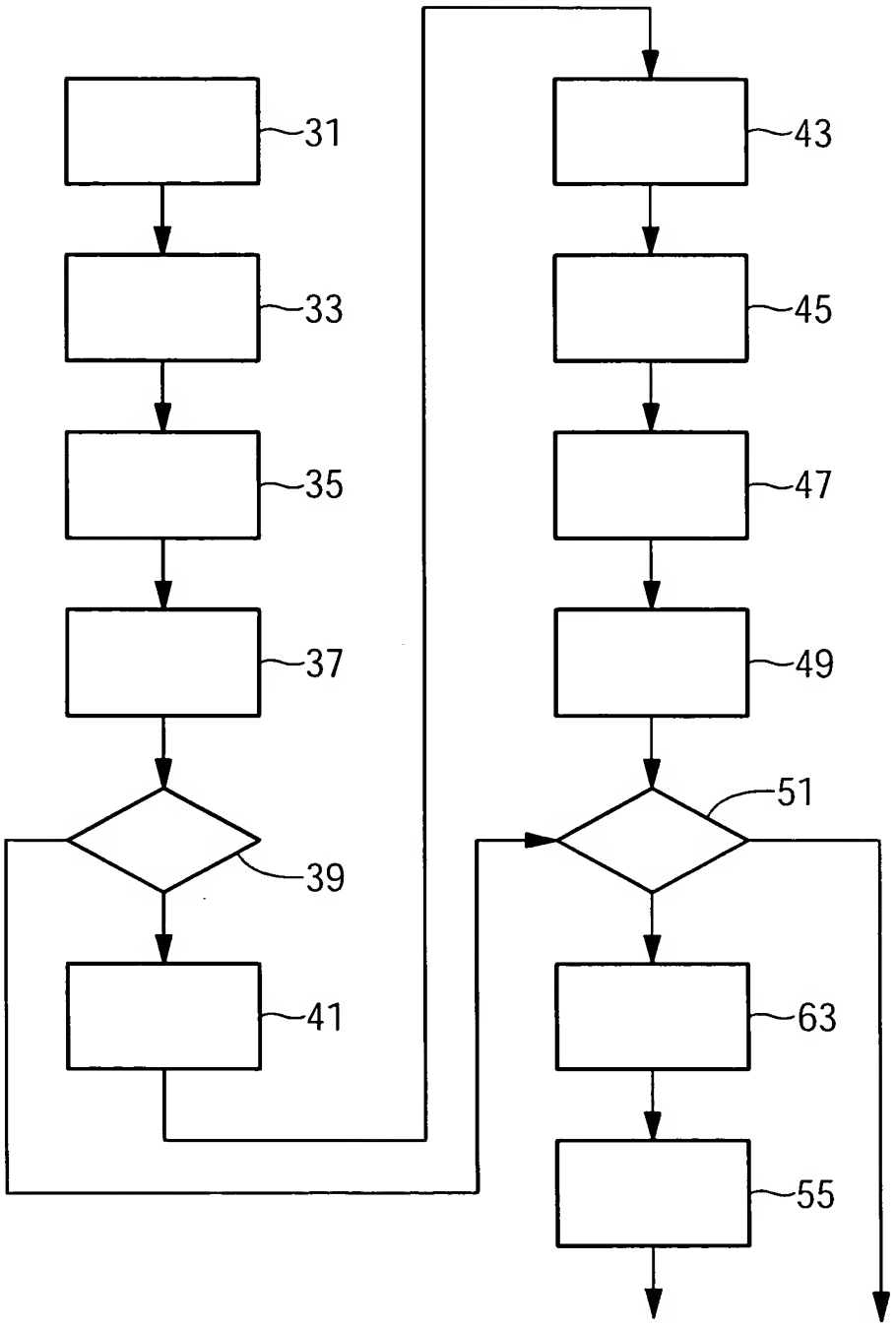

FIG 2